Kerckhoffs's principle: The security of the system should therefore be based on the key and not on the obscurity of the algorithm used. Consequently, we always assume that Eve has knowledge of the algorithm that is used to perform encryption.

Diffusion: If we change a character of the plaintext, then several characters of the ciphertext should change, and, similarly, if we change a character of the ciphertext, then several characters of the plaintext should change.

Confusion: Confusion means that the key does not relate in a simple way to the ciphertext.

CBC: $C_j = E_K(P_j \oplus C_{j-1})$ $P_j = D_K(C_j) \oplus C_{j-1}$ CFB: $O_j = L_8(E_K(X_j))$ $C_j = P_j \oplus O_j$ $X_{j+1} = R_{56}(X_j) \parallel C_j$ OFB: $O_j = L_8(E_K(X_j))$ $X_{j+1} = R_{56}(X_j) \parallel O_j$ $C_j = P_j \oplus O_j$

DES/AES: $m_0 = IP(m)$ $L_i = R_{i-1}$ $R_i = L_i \oplus f(R_{i-1}, K)$ $c = IP^{-1}(R_n L_n)$

SubByte: Removes nonlinearity. Lookup table $abcd$ row and $efgh$ column. ShiftRow and Column add diffusion. RoundKey adds confusion. All transformations must be invertible.

Affine: $D(c) = \alpha^{-1}(c - \beta) \pmod{n}$ Chosen ciphertext: Choose $0, 1$ Known plaintext: Choose x, y s.t $\gcd(x - y, n) = 1$

CRT: $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ $x = bms + ant$ where $ms + nt = 1$

Matrix inverses: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{n}$ where we need to find an inverse $ad - bc \pmod{n}$.

RSA short plaintext: (1.) $cx^{-e} \pmod{n}$ with $1 \leq x \leq 10^9$ and (2.) $y^e \pmod{n}$ with $1 \leq y \leq 10^9$ looking for $cx^{-e} \equiv y^e \pmod{n}$

Primality texting: $x^2 \equiv y^2 \pmod{n}$ but $x \neq y \pmod{n}$ then n is composite and $\gcd(x - y, n)$ is nontrivial

Miller-Rabin: $n - 1 = 2^k m$. Choose random a $b_0 \equiv a^m \equiv \pm 1 \pmod{n}$ n is prob prime

For subsequent steps $\begin{cases} b_{i+1} \equiv b_i^2 \equiv 1 \pmod{n}, & \text{n is composite } 1 < \gcd(b_i - 1, n) < n \\ b_{i+1} \equiv -1 \pmod{n}, & \text{n is probably prime} \\ \text{otherwise continue} \end{cases}$

Universal exponent is same as MR, but we assume we have some E s.t $a^E \equiv 1 \pmod{n}$

$p-1$ factoring: $b \equiv a^{B!} \pmod{n}$ nontrivial if $d = \gcd(b-1, n)$ is not 1 or n.

Diffie-Hellman: A, B choose x, y $\alpha^x \Rightarrow B$ and $\alpha^y \Rightarrow A$. Now both know $K = \alpha^{xy}$ eavesdropping can't determine without solving discrete log.

El Gamal: public key (p, α, β) $\beta = \alpha^b \pmod{p}$ private key b. Computes $r \equiv \alpha^k \pmod{p}$ and $t \equiv \beta^k m \pmod{p}$ sending (r, t). $tr^{-b} \equiv m \pmod{p}$

Pohlig-Helman: $p - 1 = \prod_i q_i^{r_i}$ $x = a_0 + a_1 q + \cdots$ $y_j \equiv y \cdot b^{-a_0 - a_1 q - \cdots}$ $y_j^{\frac{p-1}{q^{j+1}}} \equiv b^{\frac{(p-1)k}{q}} \pmod{p}$ for some k $a_i = k$ $x \equiv a_0 + a_1 q + \cdots + a_{r-1} q^{r-1} \pmod{q^r}$. If $p - 1 = kq$ where q is a large prime and k is a product of small primes, let g^k be our base.

Hash function: Given a message m, the message digest $h(m)$ can be calculated very quickly.
Given a y, it is computationally infeasible to find an m' with $h(m') = y$ preimage resistant
It is computationally infeasible to find m_1, m_2 s.t $h(m_1) = h(m_2)$ strongly collision resistant

Certificate contains: Identity, public key, digital signature from Certifying Authority. Authentication, verification, and encryption

Digital signature scheme: $\rho : \mathcal{K} \to \mathcal{K}_{pub}$, $S : \mathcal{K} \times \mathcal{P} \to \mathcal{C}$, $V : \mathcal{K}_{pub} \times \mathcal{C} \to \mathcal{P}$ $V_{\mathcal{K}_{pub}}(S_{\mathcal{K}}(m)) = m$. Easy to compute $S(\mathcal{K}, m) = c$ and $V(\mathcal{K}_{pub}, c) = m$ but very difficult to compute c without knowing $\mathcal{K}$.